Department of Engineering and Architecture
University of Parma

Network Security
Exam 10/07/2020

1) Which of the following functions is NOT a security service?

A. Data origin authentication
B. Data integrity
C. Availability
[✓ D.] Congestion control
E. Non repudiation

2) What is a *chosen-ciphertext* attack?

A. An attack scheme to a cryptographic system where the attacker can use several $\{m_i, c_i\}$ pairs, where m_i is the cleartext and $c_i=E_K(m_i)$ is the corresponding ciphertext
B. An attack scheme to a cryptographic system where the attacker can use several cleartexts $m_i=D_K(c_i)$, without knowing the key K neither the ciphertext c_i
C. An attack scheme to a cryptographic system where the attacker can select some ciphertext messages c_i and, for each c_i, she can obtain the corresponding cleartext $m_i=D_K(c_i)$
[✓ D.] An attack scheme to a cryptographic system where the attacker can select some messages m_i and, for each m_i, he can obtain the corresponding ciphertext $c_i=E_K(m_i)$

3) AES (Advanced Encryption Standard) is:

[✓ A.] A symmetric block cipher algorithm
B. An asymmetric block cipher algorithm
C. A symmetric stream cipher algorithm
D. An asymmetric stream cipher algorithm

4) Given a block cipher E in CBC mode, with block size *r* and key length *n*, let $\{m_1, c_1\}$ be a pair of plaintext and ciphertext, with message length *tr* (*t* blocks). Which is the complexity (in terms of number of calls of the function E) of a brute force attack against the secret key, supposing that in each attempt the entire message is processed.

A. $n\ 2^r$
B. $t \cdot r \cdot n$
C. $t\ 2^n$
[✓ D.] $tr\ 2^n$

5) What is the Euler's totient function $\Phi(n)$?

A. The number of prime numbers lesser than *n*
B. The multiplicative inverse of *n*
[✓ C.] The number of integers lesser than *n* that are relatively prime to *n*.
D. The smallest primitive root modulo *n*

6) X.509 is:

[✓ A.] a digital certification standard
B. a symmetric cryptography algorithm
C. a network layer secure communication protocol that uses digital certificates
D. a transport layer secure communication protocol that uses digital certificates

7) Which service is NOT provided by IPSec ESP?

A. confidentiality
B. data integrity check
[✓ C.] delivery confirmation
D. protection against replay attacks

8) What is a Key Distribution Center? Show a possible key distribution scheme that uses a KDC.

9) **Let us consider the following cleartext:**

m = `1100 0000 1100 0000`

It is sent encrypted with a symmetric block encryption algorithm $E_k(\cdot)$, with block size equal to 4bit, with key K, using OFB concatenation mode with IV=0001. The complete substitution table of $E_k(\cdot)$ with key K is reported her on the right. The resulting cipher text is:

c = `1000 0010 0001 1001 (IV=0001)`

Please indicate the value of the modified ciphertext c' and IV' such as the corresponding cleartext (when decrypted with the same key K) will be:

m'= `1100 1001 1100 0000`

plaintext	*ciphertext*
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Response:

`IV' = ?`
c = ?

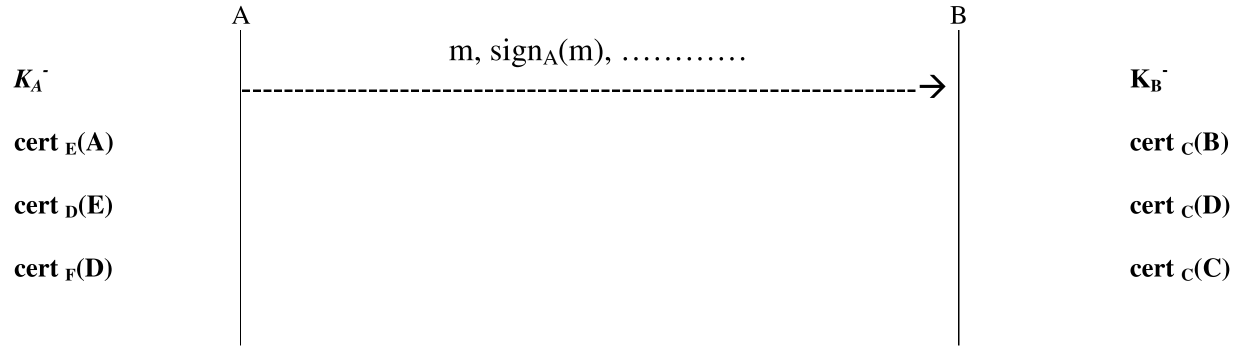
10) **Create a pair of RSA key pair K^+=<e,n> (public) and K^-=<d,n> (private), starting from the two secret prime numbers p=5, q=13, and public exponent *e*=11. For obtaining the value *d* of the private key, you can either use the Euclid's algorithm or try and test knowing that *d* is greater than 30.**
By using the private key K^- do decrypt the ciphertext *c*=2.

11) **An entity A wants to send a message *m* to B, by guaranteeing ONLY the confidentiality of the data (i.e. the message *m*). For the encryption of *m* A uses a symmetric encryption algorithm. If A and B do not share in advance any symmetric key, if both A and B have an own RSA private key (respectively K_A^- and K_B^-), and if they share the corresponding public keys K_A^+ and K_B^+, please indicate a possible scheme used by A to send the message and the scheme used by B to receive it:**

12) **Show a possible challenge-response authentication scheme that can be used by Carol to authenticate David, based on a digital signature algorithm using the private/public keys of Carol and/or David.**

13) **Show an example of authenticated Diffie-Hellman exchange between Carol (C) and David (D) that resists against MITM attack from a possible third party intruder.**

14) **An entity *A* wants to send a message *m* to *B* signed with her private key K_A^-. Consider that *A* has her own private key K^-_A, the *cert$_E$(A), cert$_D$(E),* and *cert$_F$(D)*, while *B* has *cert$_C$(B)*, *cert$_C$(D),* and *cert$_C$(C).* Which information should *A* add to message in order to let *B* verifying the signature?**



15) **The entity A wants to anonymize a message *m* to be sent to D, by using the cascade of high-latency anonymizing *Mix* nodes B and C, in such a way that A→B→C→D is the sequence of nodes that will be involved in the delivery. Assume that K^+_i and K^-_i are the public and private keys of node *i* (with *i=A,B,C,D)*. What is a possible message that A will send to B for such a purpose?**